(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 April 2004 (01.04.2004)

PCT

(10) International Publication Number
WO 2004/028071 A1

(51) International Patent Classification[7]: H04L 9/08, H04Q 7/38

(21) International Application Number: PCT/IB2002/005195

(22) International Filing Date: 25 November 2002 (25.11.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0221674.5 18 September 2002 (18.09.2002) GB

(71) Applicant *(for all designated States except US)*: NOKIA CORPORATION [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: NYBERG, Kaisa [FI/FI]; Temppelikatu 3-5 A 12, FIN-00100 Helsinki (FI). NIEMI, Valtteri [FI/FI]; Tallberginkatu 3 as 43, FIN-00180 Helsinki (FI). ASOKAN, Nadarajah [CA/FI]; Ankkurinvarsi 6 K, FIN-02320 Espoo (FI).

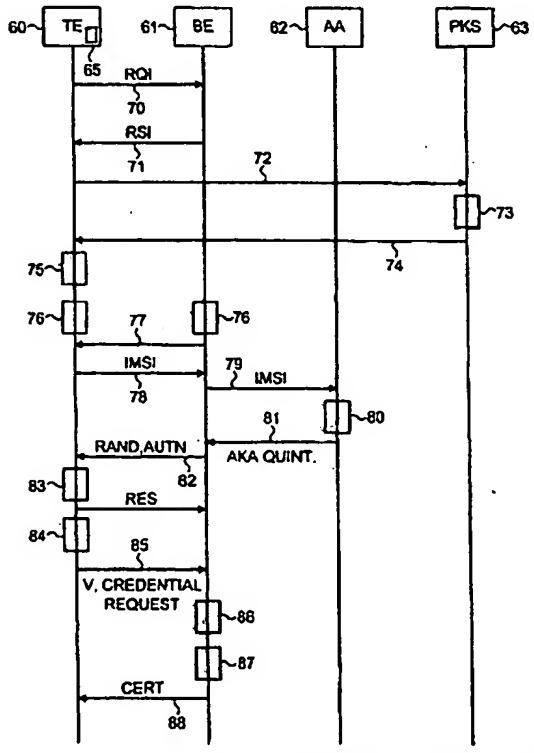
(74) Agents: SLINGSBY, Philip, Roy et al.; Page White & Farrer, 54 Doughty Street, London WC1N 2LS (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: LINKED AUTHENTICATION PROTOCOLS



(57) Abstract: A method for authenticating a terminal in a communication system, the terminal comprising identification means for applying authentication functions to input data to form response data, and the communication system being arranged to utilise a first authentication protocol for authentication of the terminal, wherein an authentication functionality and the terminal share challenge data, the terminal forms response data and a first key by applying the authentication functions to the challenge data by means of the identification means, and returns the response data to the authentication functionality, and the authentication functionality authenticates the terminal by means of the response data and can apply an authentication function to the challenge data to duplicate the first key; the method comprising; executing a second authentication protocol wherein the terminal authenticates the identity of a network entity and the terminal and the network entity share a second key for use in securing subsequent communications between the terminal and the network entity; and subsequently executing a third authentication protocol by the steps of: sharing challenge data between the network entity and the terminal; forming at the terminal test data by at least applying one of the authentication functions to the challenge data by means of the identification means; transmitting a message comprising authentication data, from the terminal to the network entity; and determining based on the authentication data whether to provide the terminal with access to a service; wherein in the determining step the terminal is provided with access to the service only if the authentication data equals a predetermined function of at least the test data and the second key.

WO 2004/028071 A1